

Number of points on a family of curves over a finite field

Thiéyacine Top*

Abstract

In this paper we study a family of curves obtained by fibre products of hyperelliptic curves. We then exploit this family to construct examples of curves of given genus g over a finite field \mathbb{F}_q with many rational points. The results obtained improve the known bounds for a few pairs (q, g) .

Key words. Curves over finite fields, jacobian varieties.

AMS subject classification. 11G20, 14G15, 14H45.

1 Introduction

Let \mathcal{C} be a (projective, non-singular and geometrically irreducible) curve of genus g defined over the finite field \mathbb{F}_q with q elements. We denote by $N_q(g)$ the maximum number of rational points on a curve of genus g over \mathbb{F}_q , namely

$$N_q(g) = \max \{ |\mathcal{C}(\mathbb{F}_q)| : \mathcal{C} \text{ is a curve over } \mathbb{F}_q \text{ of genus } g \}.$$

In the last years, due mainly to applications in Coding Theory and Cryptography (see e.g. [8]), there has been considerable interest in computing $N_q(g)$. It is a classical result that $N_q(0) = q + 1$. Deuring and Waterhouse [10], and Serre [6] computed $N_q(1)$ and $N_q(2)$ respectively. Serre also computed $N_q(3)$ for $q < 25$ and Top [7] extended these computations to $q < 100$.

For $g \geq 3$ no such general formula is known. However, Serre [6] building on earlier results by Hasse and Weil proved the following upper-bound:

$$N_q(g) \leq q + 1 + g \lfloor 2\sqrt{q} \rfloor,$$

* Université Blaise Pascal, Clermont-Ferrand, France (E-mail: thieyacine.top@math.univ-bpclermont.fr)

where $\lfloor x \rfloor$ denotes the floor part of a real number x . This bound is now called Hasse-Weil-Serre bound.

Some partial results for some specific pairs (q, g) are recorded on the website [http:// www.manypoints.org](http://www.manypoints.org) in the form $N_q(g) \in [c_1, c_2]$ or $[\dots, c_2]$, where

- c_2 is the bound given by Hasse-Weil-Serre or by "explicit formulas", or by more intricate arguments.
- c_1 is the bound given by the existence of a curve \mathcal{C} with $|\mathcal{C}(\mathbb{F}_q)| = c_1$,
- \dots when $c_1 \leq c_2/\sqrt{2}$.

Our work consists in studying geometric families of curves and studying among them those which have many points over \mathbb{F}_q . The curves we are considering are certain fibre products of hyperelliptic curves, we prove a formula for the genus and a formula for the number of rational points of such curves that depend on the polynomial f_i 's and the hyperelliptic they define. In particular by building curves of given genus explicitly, we have the following result:

Let k be an integer ≥ 1 and $q \geq 2$ be a prime power. Let I be a non-empty subset $\{1, 2, \dots, k\}$ and denote by \mathcal{I} the set of all non-empty subsets of I . Let f_1, f_2, \dots, f_k be polynomials of respective degrees d_i 's, with coefficients in the finite fields \mathbb{F}_q such that the polynomial $f_1 \times f_2 \times \dots \times f_k$ is separable. We define the polynomial

$$f_I(x) = \prod_{i \in I} f_i(x)$$

and denote by \mathcal{C}_I the hyperelliptic curve of equation $y^2 = f_I(x)$. Let $A_I = q + 1 - |\mathcal{C}_I(\mathbb{F}_q)|$. Consider now the fibre product \mathcal{C} of which an open affine subset is given by

$$\begin{cases} y_1^2 &= f_1(x) \\ &\vdots \\ y_k^2 &= f_k(x) \end{cases},$$

Let $N = |\mathcal{C}(\mathbb{F}_q)|$ where $|\mathcal{C}(\mathbb{F}_q)|$ is the number of \mathbb{F}_q -rational points on \mathcal{C} .

Theorem 1.1. *In this notation:*

- *The genus g of \mathcal{C} is given by:*

$$g = 2^{k-2}(d_1 + \dots + d_k - 4) + 1 + \delta_k,$$

with $\delta_k = 2^{k-2}$ (resp. $\delta_k = 0$) if one of the d_i 's is odd (resp. all of the d_i 's are even). There are 2^{k-1} (resp. 2^k) points at infinity if one of the d_i 's is odd (resp. all of the d_i 's are even).

- The number of \mathbb{F}_q -rational points of \mathcal{C} is given by:

$$N = q + 1 - \sum_{I \in \mathcal{I}} A_I.$$

The proof of the above theorem follows from the lemma 2.1. and the lemma 3.3. for the computation of g and $|\mathcal{C}(\mathbb{F}_q)|$ respectively. In a second part of the paper, we use Theorem 1.1 on specific examples in order to improve a current lower bounds for $N_q(g)$ for some values of (q, g) . The results we obtain are listed in Table 1.

g	q	$N_q(g)$		g	q	$N_q(g)$	
		New enter	Old			New enter	Old
5	17	48	$[\dots, 53]$	5	73	148	$[\dots, 156]$
	19	52	$[\dots, 60]$		79	156	$[\dots, 165]$
	23	62	$[\dots, 67]$		83	162	$[\dots, 172]$
	29	72	$[\dots, 80]$		89	168	$[136, 180]$
	31	76	$[\dots, 84]$		97	180	$[\dots, 193]$
	37	88	$[\dots, 96]$		5^2	64	$[\dots, 72]$
	41	94	$[\dots, 102]$		13^2	295	$[232, 300]$
	43	100	$[\dots, 106]$		17^2	454	$[376, 460]$
	47	102	$[\dots, 113]$	6	23	66	$[60, 78]$
	53	120	$[\dots, 124]$		31	84	$[80, 92]$
	59	124	$[\dots, 133]$		41	104	$[102, 114]$
	61	126	$[\dots, 137]$		59	134	$[132, 150]$
	67	136	$[\dots, 148]$	7	29	80	$[72, 100]$
	71	144	$[\dots, 152]$	8	11	46	$[42, 55]$

Table 1: The specified interval (Old) is that given by the website <http://www.manypoints.org> as of Avril 2016

2 Geometry of curves

Let k be a positive integer. Consider now the fibre product $\mathcal{C} = \mathcal{C}_{f_1 \dots f_k}$ of which an open affine subset is given by

$$\begin{cases} y_1^2 = f_1(x) \\ \vdots \\ y_k^2 = f_k(x) \end{cases},$$

where the f_i 's are coprime polynomials over \mathbb{F}_q of respective degrees d_i 's.

Lemma 2.1. *Suppose the polynomial $f(x) := \prod_i f_i(x)$ is separable, then the affine curve is smooth. The genus of the complete curve is*

$$g = 2^{k-2}(d_1 + \dots + d_k - 4) + 1 + \delta_k,$$

with $\delta_k = 2^{k-2}$ (resp. $\delta_k = 0$) if one of the d_i 's is odd (resp. all of the d_i 's are even). There are 2^{k-1} (resp. 2^k) points at infinity if one of the d_i 's is odd (resp. all of the d_i 's are even).

Proof. Smoothness follows from the jacobian criterion applied to the matrix

$$\begin{pmatrix} f'_1(x) & 2y_1 & 0 & & \\ f'_2(x) & 0 & 2y_2 & 0 & \\ & & \ddots & & \\ f'_k(x) & & & 0 & 2y_k \end{pmatrix}.$$

If none of the y_i 's is zero, there exists a minor equal to

$$2^{k-1}y_1 \dots y_{i-1}f'_i(x)y_{i+1} \dots y_k \neq 0;$$

If for some i , $y_i = 0$, then $f_i(x) = 0$ and therefore $f'_i(x) \neq 0$ and, for $j \neq i$, we have $f_j(x) \neq 0$ and there exists a minor equal to

$$2^{k-1}y_1 \dots y_{i-1}f'_i(x)y_{i+1} \dots y_k \neq 0.$$

The group $G = \{\pm 1\}^k \cong (\mathbb{Z}/2\mathbb{Z})^k$ acts in an obvious way on \mathcal{C} by

$$[\varepsilon](x, y_1, \dots, y_k) = (x, \varepsilon_1 y_1, \dots, \varepsilon_k y_k)$$

and is the Galois group of the covering

$$\phi : \mathcal{C} \rightarrow \mathbb{P}^1$$

given by

$$(x, y_1, \dots, y_k) \mapsto x.$$

The group G acts transitively on the set \mathcal{C}_∞ , of points at infinity; the inertia group is cyclic therefore is trivial or reduced to $\mathbb{Z}/2\mathbb{Z}$.

If one of the d_i 's is odd (resp. all d_i 's are even), there is ramification above $\infty \in \mathbb{P}^1$ hence we obtain $|\mathcal{C}_\infty| = 2^{k-1}$ (resp. $= 2^k$). The Riemann-Hurwitz formula applied to the morphism ϕ gives the genus, observing that ϕ is branched at every point $x = \alpha_i$ with $f_i(\alpha_i) = 0$, i.e

$$(x, y_1, \dots, y_k) = (\alpha_i, \pm \sqrt{f_1(\alpha_i)}, \dots, 0, \dots, \pm \sqrt{f_k(\alpha_i)}),$$

and possibly above ∞ .

3 Computation the number of points

We keep the same notation as before.

Definition 3.1. Let I be a non-empty subset of $\{1, \dots, k\}$, we define:

1. the polynomial $f_I(x) = \prod_{i \in I} f_i(x)$ and we denote by d_I its degree;
2. the smooth projective curve \mathcal{C}_I whose affine model is given by $v^2 = f_I(u)$;
3. we denote by g_I the genus of \mathcal{C}_I ;
4. the morphism $\phi_I : \mathcal{C} \rightarrow C_I$ given by $\phi_I(x, y_1, \dots, y_k) = (x, y_I)$ (where $y_I = \prod_{i \in I} y_i$).

We denote by \mathcal{I} the set of non-empty subsets of $\{1, \dots, k\}$.

Lemma 3.2. *The morphism*

$$\begin{aligned} \Psi : \prod_{I \in \mathcal{I}} \text{Jac}(\mathcal{C}_I) &\longrightarrow \text{Jac}(\mathcal{C}) \\ (\mathcal{C}_I)_{I \in \mathcal{I}} &\longmapsto \sum_{I \in \mathcal{I}} \phi_I^*(\mathcal{C}_I). \end{aligned}$$

is a separable isogeny.

Proof. We first verify that $\sum_{I \in \mathcal{I}} g_I = g$; indeed, if we put $d_I = \sum_{i \in I} d_i = \deg f_I$ then $g_I = \lfloor \frac{d_I - 1}{2} \rfloor$, which we may write $\frac{d_I - 1 - \varepsilon_I}{2}$ with $\varepsilon_I = 0$ or 1 .

So

$$\sum_{I \in \mathcal{I}} g_I = \sum_{I \in \mathcal{I}} \frac{d_I - 1 - \varepsilon_I}{2} = \frac{1}{2} \left(\sum_{i=1}^k d_i N_i - 2^k + 1 - \sum_I \varepsilon_I \right)$$

where N_i is the number of I 's containing i , i.e $N_i = 2^{k-1}$.

If all d_i are even, all the $\varepsilon_I = 1$ and $\frac{1}{2} \sum_I (1 + \varepsilon_I) = 2^k - 1$ and the formula follows. If at least one of d_i is odd, denote by M the number of I with d_I odd, then $\frac{1}{2} \sum_I (1 + \varepsilon_I) = 2^k - 1 - \frac{M}{2}$; we conclude by using $M = 2^{k-1}$.

The abelian varieties $\prod_{I \in \mathcal{I}} \text{Jac}(\mathcal{C}_I)$ and $\text{Jac}(\mathcal{C})$ have the same dimension. Furthermore, if $\eta_j = u^{j-1} du / v$ is a regular differential form on \mathcal{C}_I (for $1 \leq j \leq g_I$) then $\omega_{I,j} := \phi_I^*(\eta_j) = x^{j-1} dx / y_I$ is regular on \mathcal{C} and these forms are linearly independent. Indeed an equality of type:

$$\sum_I \sum_{j=1}^{g_I} \lambda_{I,j} \omega_{I,j} = 0,$$

implies

$$\sum_I P_I(x) y_{I^c} = 0,$$

where $I^c := [1, k] \setminus I$; which implies the P_I 's are zero. The differential of Ψ is an isomorphism, which proves that Ψ is a separable isogeny.

Remark. We can deduce from the previous calculation, when $k \geq 2$, that the curve C is not hyperelliptic. In fact the canonical morphism $P \mapsto (\omega_{I,j}(P))$ may be written $P \mapsto (1, x, x^2, \dots, y_1, \dots, y_k, \dots)$ thus is generically of degree 1, therefore an isomorphism (if C were hyperelliptic, it would be a morphism of degree 2).

Lemma 3.3. *Let f_1, \dots, f_k be polynomials with coefficients in the finite field \mathbb{F}_q such that the product $f_1 \dots f_k$ is separable, and let C be the associated curve. Let $A_I = q + 1 - |C_I(\mathbb{F}_q)|$ then,*

$$|C(\mathbb{F}_q)| = q + 1 - \sum_{I \in \mathcal{I}} A_I.$$

Proof. The abelian varieties $\text{Jac}(C)$ and $\prod_I \text{Jac}(C_I)$ are \mathbb{F}_q -isogenous therefore have the same number of points on \mathbb{F}_{q^m} . If

$$|C(\mathbb{F}_{q^m})| = q^m + 1 - (\beta_1^m + \dots + \beta_{2g}^m)$$

then

$$|\text{Jac}(C)(\mathbb{F}_{q^m})| = \prod_{1 \leq i \leq 2g} (1 - \beta_i^m)$$

and if

$$|C_I(\mathbb{F}_{q^m})| = q^m + 1 - ((\alpha_1^{(I)})^m + \dots + (\alpha_{2g}^{(I)})^m)$$

then

$$|\text{Jac}(C_I)(\mathbb{F}_{q^m})| = \prod_{1 \leq i \leq 2g} (1 - (\alpha_i^{(I)})^m)$$

and thus therefore

$$|\text{Jac}(C)(\mathbb{F}_{q^m})| = \prod_I |\text{Jac}(C_I)(\mathbb{F}_{q^m})| = \prod_I \prod_j (1 - (\alpha_j^{(I)})^m),$$

$$|C_I(\mathbb{F}_{q^m})| = q^m + 1 - ((\alpha_1^{(I)})^m + \dots + (\alpha_{2g}^{(I)})^m) = q^m + 1 - \sum_I \sum_{1 \leq j \leq g_I} (\alpha_j^{(I)})^m,$$

and, in particular , for $m = 1$, we get

$$|C(\mathbb{F}_q)| = q + 1 - \sum_I \sum_{1 \leq j \leq g_I} \alpha_j^{(I)} = q + 1 - \sum_{I \in \mathcal{I}} A_I.$$

4 Numerical examples

Examples of genus- g curves $y_1^2 = f_1$, $y_2^2 = f_2$ over \mathbf{F}_q having many points. The meaning of the quantities A_1 , A_2 , A_3 , and N is explained in the text. The following examples improve some results listed on the website <http://www.manypoints.org> and were computed using the computer algebra package Magma.

$q = 17$	$f_1 = x^4 + x^3 + 16x^2 + 15x + 1$ $f_2 = x^4 + 13x^3 + 16x^2 + 15$	$A_1 = -8$ $A_2 = -6$ $A_3 = -16$	$N = 48 \in [\dots, 53]$
$q = 19$	$f_1 = x^4 + x^3 + 18x^2 + 13x + 14$ $f_2 = x^4 + 4x^3 + 18x^2 + 7x + 12$	$A_1 = -8$ $A_2 = -8$ $A_3 = -16$	$N = 52 \in [\dots, 60]$
$q = 23$	$f_1 = x^4 + 19x^3 + 7$ $f_2 = x^3 + x + 11$	$A_1 = -9$ $A_2 = -9$ $A_3 = -18$	$N = 60 \in [\dots, 67]$
$q = 29$	$f_1 = x^4 + x^3 + 28x^2 + 28x + 18$ $f_2 = x^4 + 27x^3 + 27x^2 + 28x + 15$	$A_1 = -10$ $A_2 = -10$ $A_3 = -22$	$N = 72 \in [\dots, 80]$
$q = 31$	$f_1 = x^4 + x^3 + 30x^2 + 30x + 10$ $f_2 = x^4 + 30x^3 + 5x^2 + 19x + 14$	$A_1 = -11$ $A_2 = -10$ $A_3 = -23$	$N = 76 \in [\dots, 84]$
$q = 37$	$f_1 = x^4 + x^3 + 35x^2 + 32x + 1$ $f_2 = x^4 + 11x^3 + 29x^2 + 13x + 29$	$A_1 = -12$ $A_2 = -12$ $A_3 = -26$	$N = 88 \in [\dots, 96]$
$q = 41$	$f_1 = x^4 + x^3 + 40x^2 + 40x + 36$ $f_2 = x^4 + 23x^3 + 10x^2 + 20x + 36$	$A_1 = -12$ $A_2 = -11$ $A_3 = -29$	$N = 94 \in [\dots, 102]$
$q = 43$	$f_1 = x^4 + x^3 + 41x^2 + 34x + 1$ $f_2 = x^4 + 12x^3 + 17x^2 + 41x + 38$	$A_1 = -13$ $A_2 = -13$ $A_3 = -30$	$N = 100 \in [\dots, 106]$
$q = 47$	$f_1 = x^4 + 25x^3 + x^2 + 2x + 31$ $f_2 = x^3 + x + 38$	$A_1 = -12$ $A_2 = -13$ $A_3 = -29$	$N = 102 \in [\dots, 113]$
$q = 53$	$f_1(x) = x^4 + x^3 + 52x^2 + 47x + 1$ $f_2(x) = x^4 + 16x^3 + 36x^2 + 18x + 46$	$A_1 = -14$ $A_2 = -14$ $A_3 = -38$	$N = 120 \in [\dots, 124]$

$q = 59$	$f_1(x) = x^4 + x^3 + 54x^2 + 6x + 1$ $f_2(x) = x^4 + 13x^3 + 22x^2 + 3x + 9$	$A_1 = -15$ $A_2 = -15$ $A_3 = -34$	$N = 124 \in [..., 133]$
$q = 61$	$f_1(x) = x^4 + x^3 + 58x^2 + 18x + 1$ $f_2(x) = x^4 + 27x^3 + 5x^2 + 47x + 28$	$A_1 = -15$ $A_2 = -14$ $A_3 = -35$	$N = 126 \in [..., 137]$
$q = 67$	$f_1(x) = x^4 + x^3 + 66x^2 + 57x + 1$ $f_2(x) = x^4 + 2x^3 + 49x^2 + 24x + 1$	$A_1 = -16$ $A_2 = -16$ $A_3 = -36$	$N = 136 \in [..., 148]$
For $q = 71$	$f_1(x) = x^4 + x^3 + x^2 + 44x + 1$ $f_2(x) = x^4 + 9x^3 + 8x^2 + 21x + 64$	$A_1 = -16$ $A_2 = -16$ $A_3 = -40$	$N = 144 \in [..., 152]$
For $q = 73$	$f_1(x) = x^4 + x^3 + 66x^2 + 57x + 1$ $f_2(x) = x^4 + 2x^3 + 49x^2 + 24x + 1$	$A_1 = -17$ $A_2 = -17$ $A_3 = -40$	$N = 148 \in [..., 156]$
For $q = 79$	$f_1(x) = x^4 + x^3 + 3x^2 + 7x + 1$ $f_2(x) = x^4 + 4x^3 + 5x^2 + 24x + 68$	$A_1 = -16$ $A_2 = -16$ $A_3 = -36$	$N = 156 \in [..., 165]$
For $q = 83$	$f_1(x) = x^4 + x^3 + x^2 + 5x + 1$ $f_2(x) = x^4 + 72x^3 + 54x^2 + 29x + 36$	$A_1 = -18$ $A_2 = -16$ $A_3 = -44$	$N = 162 \in [..., 172]$
For $q = 89$	$f_1(x) = x^4 + x^3 + 3x^2 + 7x + 1$ $f_2(x) = x^4 + 4x^3 + 5x^2 + 24x + 68$	$A_1 = -16$ $A_2 = -16$ $A_3 = -36$	$N = 168 \in [136, 180]$
$q = 97$	$f_1(x) = x^4 + 8x^3 + 3x^2 + 23x + 1$ $f_2(x) = x^4 + 9x^3 + 63x^2 + 28x + 91$	$A_1 = -19$ $A_2 = -19$ $A_3 = -44$	$N = 180 \in [..., 193]$
$q = 5^2$	$f_1(x) = x^4 + x^2 + rx$ $f_2(x) = x^4 - 2rx^3 + rx + 2$ with $r^2 + r + 1 = 0$	$A_1 = -9$ $A_2 = -9$ $A_3 = -24$	$N = 68 \in [..., 72]$
$q = 13^2$	$f_1(x) = (x - 2)(x^2 - 2)$ $f_2(x) = x^4 - 4x^2 + 1$	$A_1 = -26$ $A_2 = -21$ $A_3 = -78$	$N = 295 \in [232, 300]$
$q = 17^2$	$f_1(x) = (x + 2)(x + 10)(x^2 + 6)$ $f_2(x) = (x^2 + 10)(x^2 + 6x + 3)$	$A_1 = -33$ $A_2 = -29$ $A_3 = -102$	$N = 454 \in [376, 460]$

Table 2: Examples of genus-5.

$q = 23$	$f_1(x) = x^5 + 12x^4 + 19x^3 + x + 2$ $f_2(x) = x^3 + 12x^2 + 18x + 4$	$A_1 = -13$ $A_2 = -9$ $A_3 = -20$	$N = 66 \in [60, 78]$
$q = 31$	$f_1(x) = x^5 + 6x^4 + 4x^3 + 4x^2 + 17x + 16$ $f_2(x) = (x)^3 + 13x^2 + 15x + 13$	$A_1 = -19$ $A_2 = -11$ $A_3 = -22$	$N = 84 \in [80, 92]$
$q = 41$	$f_1(x) = x^5 + 31x^4 + 11x^3 + 14x^2 + 35x + 40$ $f_2(x) = x^3 + 23x^2 + 5x + 17$	$A_1 = -23$ $A_2 = -12$ $A_3 = -27$	$N = 104 \in [102, 114]$
$q = 59$	$f_1(x) = x^5 + 57x^4 + 17x^3 + 48$ $f_2(x) = x^3 + 2x + 22$	$A_1 = -25$ $A_2 = -15$ $A_3 = -34$	$N = 134 \in [132, 150]$

Table 3: Examples of genus-6 .

$q = 29$	$f_1(x) = x^6 + 9x^5 + 3x^4 + 1$ $f_2(x) = x^4 + 13x^3 + 28x^2 + 12x + 1$	$A_1 = -46$ $A_2 = -40$ $A_3 = -54$	$N = 80 \in [72, 100]$
----------	--	---	------------------------

Table 4: Examples of genus-7 .

Acknowledgements

We thank Professor Marc Hindry (Paris 7), the mathematics lab of the University Blaise Pascal in particular Nicolas Billerey and Marusia Rebelledo.

References

- [1] Everett W. Howe. New bounds on the maximum number of points on genus-4 curves over small finite fields, Arithmetic, Geometry, Cryptography and Coding Theory (Y. Aubry, C. Ritzenthaler, and A. Zykin, eds.), Contemporary Mathematics 574, in American Mathematical Society, Providence, RI, 2012, pp 69-86.
- [2] Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. J. Fac. Sci. Univ. Tokyo Sect. IA Math., 28(3):721–724 (1982), 1981.

- [3] Tetsuo Kodama, Jaap Top, and Tadashi Washio. Maximal hyperelliptic curves of genus three. *Finite Fields Appl.*, 15(3):392–403, 2009.
- [4] Stephen Meagher and Jaap Top. Twists of genus three curves over finite fields. *Finite Fields and their Appl.*, 16:347–368, 2010.
- [5] Jean-Pierre Serre. Nombres de points des courbes algébriques sur \mathbb{F}_q . In *Seminar on number theory, 1982–1983 (Talence, 1982/1983)*, pages Exp. No. 22, 8. Univ. Bordeaux I, Talence, 1983.
- [6] Jean-Pierre Serre. Rational points on curves over finite fields. Unpublished notes by F.Q. Gouvêa of lectures at Harvard. 1985.
- [7] Jaap Top. Curves of genus 3 over small finite fields. *Indag. Math. (N.S.)*, 14(2):275–283, 2003.
- [8] Michael Tsfasman, Serge Vladut, and Dmitry Nogin. Algebraic geometric codes: basic notions, volume 139 of *Mathematical Survey and Monographs*. American Mathematical Society, Providence, RI, 2007.
- [9] Gerard van der Geer and Marcel van der Vlugt. Tables of curves with many points. *Math. Comp.*, 69(230):797–810, 2000.
- [10] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. Ecole Norm. Sup. (4)*, 2:521–560, 1969.